Winter 12-1-2010

A Hybrid Approach For Information Systems Security Risk Assessment In Electronic Business

Nan Feng

Minqiang Li

A HYBRID APPROACH FOR INFORMATION SYSTEMS SECURITY RISK ASSESSMENT IN ELECTRONIC BUSINESS

Nan Feng, Minqiang Li
Department of Information Management and Management Science, School of Management, Tianjin University, Tianjin, China.
E-mail: tju_fengnan@yahoo.com.cn

Abstract

In electronic business environment, it is critical for an enterprise to assess information systems security (ISS) risks. In this paper, we propose a hybrid approach for ISS risk assessment in e-business. Given there is a great deal of uncertainty in the ISS risk assessment in e-business environment, in the hybrid approach, we combine the evidence theory with fuzzy sets to deal with the uncertain evidence found in the ISS risk assessment. The proposed approach provides a new way to define the basic belief assignment in fuzzy measure. Moreover, the approach also provides a method of testing the evidential consistency, which can reduce the uncertainty derived from the conflicts of evidence. Finally, the approach is further demonstrated and validated via a case study, in which sensitivity analysis is employed to validate the reliability of the proposed approach.

1. Introduction

In electronic business, the dependence on information systems (IS) has increased in current business environments where a variety of transactions involving trading of goods and services are accomplished electronically [1, 2]. Increasing organizational dependence on the IS in e-business has led to a corresponding increase in the impact of information systems security (ISS) abuses. Therefore, the ISS is a critical issue that has attracted much attention from both researchers and practitioners in e-business.

In order to prevent security breaches, businesses use controls (and various countermeasures) to safeguard their assets from various patterns of threats by identifying the IS assets that are vulnerable to threats. But, even in the presence of controls, the assets are often not fully protected from threats because of inherent control weaknesses. Thus, the risk assessment is a critical step for the ISS risk management in e-business [3].

In practice, the ISS risk assessment is quite complex and full of the uncertainty as well [4]. The uncertainty, existing in the risk assessment in e-business, has been the primary factor that influences the effectiveness of the ISS risk assessment to a large extent. Therefore, in order to deal with the incompleteness and vagueness of information, the uncertainty must be taken into account in the ISS risk assessment. However, most existing approaches applied to the ISS risk assessment have some drawbacks on handling uncertainty in the process of assessment.

To address these aforementioned issues in e-business, we propose a hybrid approach that combines the evidence theory with fuzzy sets for ISS risk assessment in electronic business. In this paper, the approach provides a new way to define the basic belief assignment in fuzzy measure for dealing with the uncertain evidence found in the ISS risk assessment in e-business. Moreover, we discuss a process of testing the evidential consistency in the ISS risk assessment in e-business. This process can effectively reduce the uncertainty derived from the conflicts of evidence provided by experts.

The rest of this paper is organized as follows: Section 2 reviews the related works on ISS risk assessment in e-business. In the next section, we discuss the procedure of the hybrid approach for ISS risk assessment in detail in Section 3. Then, the proposed approach is further demonstrated and validated in Section 4 via a case study. Finally, we summarize our contributions and present our further research.

2. Literature Review

2.1 Related Work

The existing approaches for the ISS risk assessment in e-business can be grouped into three major categories: the quantitative approaches, the qualitative approaches, and the combination of quantitative and qualitative approaches.

The quantitative approaches consider the IS risk exposure as a function of the probability of a threat and the expected loss due to the vulnerability of the organization to this threat [5, 6]. The stochastic dominance (SD) approach [7] focuses on answering the specific question of what contingency plan should be used to prevent losses if a disaster occurs. To achieve this goal, the SD compares the costs associated with various backup and recovery options during the entire disaster recovery process in all areas of the organization. However, it fails to provide guidance on how to

assess the failure of multiple controls pertaining to a single threat or how to assess the failure and the impact of a single control on multiple threats. The proposed approach in this paper provides a structure to the ISS risk assessment process by decomposing risk into its subcomponents and identifying relevant controls and their interrelationships. The approach based on neural networks [8] consists of five phases: network parameter initialization, input the training sample and the expectation output, network self-learning, forward propagation, and back propagation. If the error function value is smaller than the pre-established value, the network learning is stopped, otherwise turn to the second phase. While this approach has the intelligent features such as the self-learning and the acquisition of knowledge, which is different from the conventional methods, it is very difficult to get a large numbers of training samples for network self-learning in the process of the risk assessment in e-business. The modular attack trees [9] approach is specified as parametric constraints, which allow quantifying the probability of security breaches that occur due to internal component vulnerabilities as well as vulnerabilities in the component's deployment environment. Based on the attack probabilities and the structure of the modular attack trees, security risks can be estimated for the information system. But, this approach has the difficulties capturing the uncertainty in the ISS risk environment dealing with the existence of the incompleteness and vagueness of information.

In the qualitative approaches, such as the logic analysis [10] and the Delphi method [11], the probability data is not required and only the estimated potential loss is used. Since the qualitative analysis depends to a great extent on the analyst's experience, both the process and the result of the security risk assessment are relatively subjective [12].

As information systems have become more complex in e-business, neither quantitative nor qualitative approaches can properly model the assessment process alone. Therefore, the comprehensive approaches combining both the quantitative and the qualitative approaches are needed [13, 14]. The approach using the Bayesian Networks (BNs) [15, 16, 17] provides an objective and visible support for risk analysis. It consists of three phases: the BN initialization (define the structure and the set of conditional probability distributions), the risk monitoring, and the risk analysis. Using new evidence obtained from information system, this approach can continually estimate risk probability and identify the sources of risk. The approach based on the fuzzy comprehensive evaluation (FCE) [18, 19, 20] is a mathematical method to comprehensively evaluate the ISS risks by using fuzzy set theory of fuzzy mathematics. Although this approach is good at processing the ambiguous information by simulating the characteristic of human in making the judgment, it is not capable to provide the graphical relationships among various ISS risk factors using flow charts or diagrams. The proposed approach in this paper consists of the graphical representation of relevant constructs through an evidential diagram, which can fully capture the complexity of multiple controls dealing with one threat and also that of one control dealing with multiple threats. In addition, both the above approaches are suffering from the uncertainty derived from the conflicts of evidence provided by experts. In this paper, we propose a method of testing the evidential consistency, which can reduce the uncertainty derived from the conflicts of evidence.

In this paper, we combine the evidence theory with fuzzy sets to model the uncertainty involved in the ISS risk assessment in e-business. In addition to representing uncertainties, the present approach allows the decision maker to develop an evidential diagram to assess the ISS risk that contains various variables such as the IS assets, the related threats, and the corresponding countermeasures in e-business. Next, the decision maker can input his or her judgments about the presence or absence of threats and the impact of countermeasures on the corresponding threats according to belief functions.

2.2 Evidence Theory

The evidence theory, also called the Dempster-Shafer's theory, has often been applied in the reasoning under uncertainty [21, 22].

Suppose we have a decision problem with n possible elements or states of nature forming a mutually exclusive and collectively exhaustive set. This set is called the frame of discernment represented by Θ. The power set of Θ containing all the possible subsets of Θ, represented as $P(\Theta)$.

A basic belief assignment (BBA) is a function from $P(\Theta)$ to [0, 1] defined by:

$$\begin{aligned} m &: P(\Theta) \to [0,1] \\ A &\mapsto m(A) \end{aligned}, \tag{1}$$

where A is an element of $P(\Theta)$. In addition, it satisfies the following conditions:

$$\sum_{A \in P(\Theta)} m(A) = 1, \tag{2}$$

$$m(\varnothing) = 0. \tag{3}$$

Basically, the BBA pertaining to a statement measures the degree of belief directly assigned to the statement based on the evidence.

Dempster's rule is the fundamental rule for combining two or more items of evidence in the belief function framework. For simplicity, let us illustrate Dempster's rule for only two items of

evidence. In general, if m_1 and m_2 are two BBAs representing two independent items of evidence pertaining to Θ, then the combined BBAs for a subset A of frame Θ using Dempster's rule is given by

$$m(A) = K^{-1} \sum_{B \cap C = A} m_1(B) m_2(C), \quad (4)$$

where $K = 1 - \sum_{B \cap C = \varnothing} m_1(B) m_2(C)$, which represents the renormalization constant. The second term in K represents the conflict.

3. The Hybrid Approach for ISS Risk Assessment

The hybrid approach consists of four phases: (a) establish the ISS index system and quantify the index weights, (b) construct the evidential diagram, (c) compute the BBAs for the assertions in the evidential diagram, (d) test the evidential consistency. Each phase is discussed in detail as follows. And, the procedure of the approach is given in Figure 1.

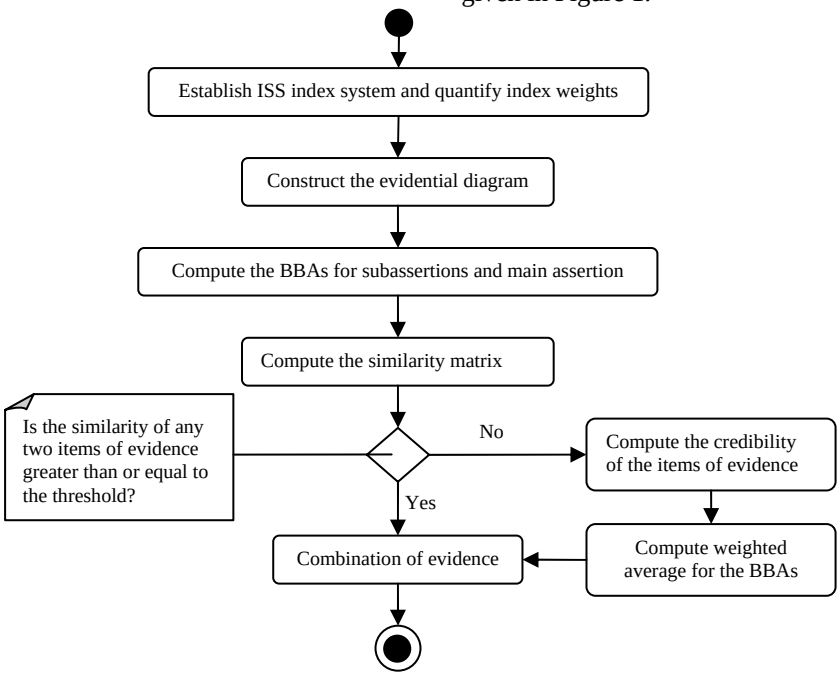

Figure 1. The hybrid approach procedure.

3.1 Establish the ISS Index System and Quantify Index Weights

The ISS index system is based on the risk analysis, which includes the identification of vulnerabilities and threats, the analysis of the losses arising from the threats acting on vulnerabilities [23]. Based on the ISS risk analysis for an on-line securities company (see Section 4), we have established the index system (see Table 1).

For quantifying the index weights, six information system experts, two of which are also this company's IT managers, were invited to fill in the questionnaires about the comparison table of factor weights. And then, we have quantified the index weights using the method in reference [24]. This method can effectively reduce the uncertainty in the process of quantifying index weights [24].

Table 1. ISS risk index system and index weights.

First level index	Second level indexes	Weights	Third level indexes	Weights
ISS risk	ISS vulnerabilities	0.262	Hardware defects	0.134
			Software defects	0.369
			Network vulnerabilities	0.284
			Communication protocol vulnerabilities	0.213
	ISS threat	0.246	Deletion or loss of information	0.264
			Breach of network resources	0.303
			Information abuse	0.229
			Information leakage	0.204
	Assets loss	0.206	Tangible assets loss	0.512
			Intangible assets loss	0.488
	Capability loss	0.173	Service interruption	0.681
			Service delay	0.184
			Service weakening	0.135
	Cost of system recovery	0.113	Cost of information recovery	0.338
			Cost of service recovery	0.662

3.2 Construct the Evidential Diagram

An evidential diagram consists of assertions, evidence, and their interrelationships. Assertions include the main assertion and subassertions. The

main assertion is the highest-level assertion; the subassertions are lower-level assertions. Relationships between assertions (e.g., between the main assertion and subassertions, and between higher-level subassertions and lower-level subassertions) need to be defined using logical relationships such as "and" and "or." And evidence represents the information that supports or negates assertions.

In this paper, the evidential diagram is derived from the ISS index system. Suppose a manager is interested in evaluating the ISS risk involved in the ISS vulnerabilities. The corresponding evidential diagram is given in Figure 2, which is a part of the evidential diagram for the main assertion "ISS risk" in a securities company. In Figure 2, the rounded boxes represent assertion nodes. And evidence nodes are represented by rectangular boxes in the evidential diagrams. Numbers in parentheses represent weights. Evidence nodes are connected to the corresponding assertion(s) that they directly pertain to. For instance, the evidence "E1.1.1 Vulnerabilities of hardware protection measures" directly pertains to assertion "A1.1 ISS vulnerabilities" and thus it is connected to that assertion.

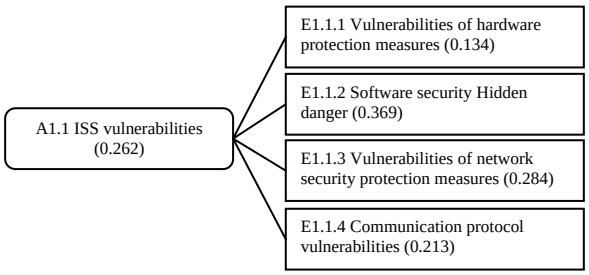

Figure 2. Hypothetical evidential diagram for ISS vulnerabilities.

3.3 Compute the BBAs for Assertions in Evidential Diagram

In e-business, the evidence is generally described in fuzzy form in ISS risk assessment [25]. For this reason, we introduce fuzzy sets to evidence space and define the BBAs in fuzzy measure so that we can further reduce the degree of uncertainty in ISS risk assessment.

In this section, we combine evidence theory with fuzzy sets to compute the BBAs in fuzzy form as follow.

We assume that E is an evidence space, $E = \{e_1, e_2,\ldots, e_n\}$, and $\Theta = \{a_1, a_2,\ldots, a_m\}$.

Definition 1. Let $\tilde{F}$ be a fuzzy set on E, $u_{\tilde{F}}: E \to [0,1], e \to u_{\tilde{F}}(e)$. Then $u_{\tilde{F}}$ is called membership function for $\tilde{F}$, and $u_{\tilde{F}}(e)$ is called a membership from e to $\tilde{F}$. Let $F(E)$ be a set composed of fuzzy subsets of E, then $F(E)$ is called the fuzzy power set of E.

Definition 2. Let $\tilde{F}_1$、$\tilde{F}_2 \in F(E)$. Then $u_{\tilde{F}_1 \cup \tilde{F}_2}$ and $u_{\tilde{F}_1 \cap \tilde{F}_2}$ are defined as:

(1) $u_{\tilde{F}_1 \cup \tilde{F}_2}(e) \triangleq u_{\tilde{F}_1}(e) \vee u_{\tilde{F}_2}(e)$;

(2) $u_{\tilde{F}_1 \cap \tilde{F}_2}(e) \triangleq u_{\tilde{F}_1}(e) \wedge u_{\tilde{F}_2}(e)$.

Definition 3. If the following conditions hold:

(1) $E \in F(E)$;

(2) If $\tilde{F}_1$、$\tilde{F}_2$、$\cdots$、$\tilde{F}_n \in F(E)$, then $\bigcup_{i=1}^{n} \tilde{F}_i \in F(E)$,

then $F(E)$ is called a fuzzy additive set.

Definition 4. Let $P(e_i)$ be a probability density function on E, $F(E)$ a fuzzy additive set on E, and w_i a weight of e_i. If $\tilde{F} \in F(E)$, then the probability $P(\tilde{F})$ can be defined as:

$$P(\tilde{F}) = \sum_{i=1}^{n} u_{\tilde{F}}(e_i) w_i P(e_i) \quad i = 1, 2, \cdots, n \tag{5}$$

Definition 5. Set up a mapping $\Gamma: F(E) \to \Theta$. Let A_j be an element of $P(\Theta)$. If $\exists \tilde{F}_k \in F(E), s.t.\ \Gamma(\tilde{F}_k) = A_j$ (j = 1, 2, ... , 2^m; k = 1, 2, … , l), then the mapping $\Gamma[P]: \Theta \to [0,1]$ is defined as:

$$\Gamma[P](A_j) = \begin{cases} \dfrac{P\left(\bigcup\limits_{\substack{\tilde{F}_k \in F(E) \\ \Gamma(\tilde{F}_k) = A_j}} \tilde{F}_k\right)}{M} & A_j \neq \varnothing \\ 0 & A_j = \varnothing \end{cases}, \tag{6}$$

where $M = \sum\limits_{\substack{A_j \in P(\Theta) \\ A_j \neq \varnothing}} P\left(\bigcup\limits_{\substack{\tilde{F}_k \in F(E) \\ \Gamma(\tilde{F}_k) = A_j}} \tilde{F}_k\right)$. Let $\tilde{B} = \left(\bigcup\limits_{\substack{\tilde{F}_k \in F(E) \\ \Gamma(\tilde{F}_k) = A_j}} \tilde{F}_k\right)$, we have:

$$\begin{aligned} M &= \sum_{\substack{A_j \in P(\Theta) \\ A_j \neq \varnothing}} \sum_{i=1}^{n} u_{\tilde{B}}(e_i) w_i P(e_i) \\ &= \sum_{\substack{A_j \in P(\Theta) \\ A_j \neq \varnothing}} \sum_{i=1}^{n} \max_{\Gamma(\tilde{F}_k) = A_j} \left\{u_{\tilde{F}_k}(e_i)\right\} w_i P(e_i) \end{aligned}. \tag{7}$$

Based on above definitions, we can propose the following proposition:

Proposition 1. $\Gamma[P](A_j)$ is a BBA on Θ.

Proof:

If $A_j = \varnothing$, then $\Gamma[P](\varnothing) = 0$;

If $A_j \neq \varnothing$, we have:

$$\sum_{A_j \in P(\Theta)} \Gamma[P](A_j) = \sum_{A_j \in P(\Theta)} \frac{P\left(\bigcup_{\substack{\tilde{F}_k \in F(E) \\ \Gamma(\tilde{F}_k)=A_j}} \tilde{F}_k \right)}{M} = \frac{1}{M} \sum_{A_j \in P(\Theta)} P\left(\bigcup_{\substack{\tilde{F}_k \in F(E) \\ \Gamma(\tilde{F}_k)=A_j}} \tilde{F}_k \right) = 1 .$$

The proposition is proved.

According to above definitions and Proposition 1, the mass function, i.e. $\Gamma[P](A_j)$, can effectively meet the requirement to deal with the situation where there is the uncertain evidence in the process of ISS risk assessment in e-business.

3.4 Test the Evidential Consistency

In the uncertain reasoning by evidence theory, if an item of evidence is in conflict with other(s), the reasoning result would not be sound [26]. To illustrate the conflict of evidences, we give an example as follow.

Assumed that the frame Θ is $\{a, b, c\}$. If the BBAs for an item of evidence A are $m_1(a) = 0.99$ and $m_1(b) = 0.01$, and the BBAs for an item of evidence B are $m_2(b) = 0.01$ and $m_2(c) = 0.99$, then we have $m(a) = m(c) = 0$ and $m(b) = 1$ by combining of evidences. Although the supports of A and B for event b is very low, the reasoning result is that the event b is true. It is obviously not reasonable. Therefore, the testing evidential consistency has important significance for the ISS risk assessment based on evidence theory.

Furthermore, we discuss the process of testing evidential consistency in detail next.

Definition 6. Let $S_{P(\Theta)}$ be the space generated by all the subsets of Θ. A BBA is a vector $\vec{m}$ of $S_{P(\Theta)}$ with coordinates $m(A_i)$ such that

$$\sum_{i=1}^{2^N} m(A_i) = 1 \; and \; m(A_i) \geq 0, i = 1, \ldots, 2^N , \quad (8)$$

where $A_i \in P(\Theta)$.

Assume that m_1 and m_2 are two BBAs on the same frame of discernment Θ. According to reference [22], the distance between m_1 and m_2 is:

$$d_{BPA}(m_1, m_2) = \sqrt{\frac{1}{2}\left(\| \vec{m}_1 \|^2 + \| \vec{m}_2 \|^2 - 2\langle \vec{m}_1, \vec{m}_2 \rangle \right)} \quad (9)$$

where $\langle \vec{m}_1, \vec{m}_2 \rangle$ is the scalar product defined by

$$\langle \vec{m}_1, \vec{m}_2 \rangle = \sum_{i=1}^{2^N} \sum_{j=1}^{2^N} m_1(A_i) m_2(A_j) \frac{|A_i \cap A_j|}{|A_i \cup A_j|}, \quad (10)$$

with A_i , $A_j \in P(\Theta)$ for $i, j = 1, \ldots, 2^N$. $\| \vec{m} \|^2$ is then the square norm of $\vec{m}$:

$$\| \vec{m} \|^2 = \langle \vec{m}, \vec{m} \rangle . \quad (11)$$

Based on the evidential distance, we can further define the similarity of two BBAs:

$$S(m_i, m_j) = 1 - d_{BPA}(m_i, m_j) \quad i, j = 1, 2, \cdots, n . \quad (12)$$

Thus the result can be represented by a similarity matrix:

$$SM = \begin{bmatrix} 1 & S_{12} & \cdots & S_{1j} & \cdots & S_{1n} \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ S_{i1} & S_{i2} & \cdots & S_{ij} & \cdots & S_{in} \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ S_{n1} & S_{n2} & \cdots & S_{nj} & \cdots & 1 \end{bmatrix} .$$

Furthermore, the support for a BBA m_i is:

$$Sup(m_i) = \sum_{\substack{j=1 \\ j \neq i}}^{n} S(m_i, m_j) \quad i, j = 1, 2, \cdots, n . \quad (13)$$

The support for the BBA m_i, i.e. $Sup(m_i)$, reflects the degree of the support of other BBAs. Based on it, we have the credibility $C(m_i)$:

$$C(m_i) = \frac{Sup(m_i)}{\sum_{i=1}^{n} Sup(m_i)} \quad i, j = 1, 2, \cdots, n . \quad (14)$$

Obviously, $\sum_{i=1}^{n} C(m_i) = 1$. Therefore, $C(m_i)$ can represent the weight of the BBA m_i.

In the process of testing evidential consistency in the ISS risk assessment, a threshold value ξ can be set according to the actual situations. If the similarity of any two items of evidence is greater than or equal to the threshold value ξ, then it is considered that the existing items of evidence are consistent. In contrast, if the similarity is lesser than ξ, we have to adjust the existing items of evidence.

For the evidential adjustment, if an item of evidence is supported by other items of evidence, then it has a higher credibility and we assign a larger weight for it in evidence combination; In contrast, if an item of evidence is in conflict with other items of evidence, then its credibility and weight should be smaller. The steps of the evidential adjustment are as follows:

Step 1. Obtain the credibility of the items of evidence.

Based on Eqs. (13) and (14), we can obtain the credibility of the items of evidence.

Step 2. Weighted average for BBAs of the items of evidence

Let us treat the credibility as the weight of evidence. Then, we weighted average for BBAs of the items of evidence.

Step 3. Combine the weighted average evidence.

According to reference [27], if there are n items of evidence, we combine the weighted average evidence n-1 times using Eq. (4).

4. Case Analysis and Evaluation

In order to further validate the proposed approach, we used it in assessing an actual company's information systems. This company is a Chinese financial services firm providing on-line services in securities trading and sales.

In this section, we first demonstrate the presented approach via a case study according to the procedure of Section 3. Then sensitivity analysis is employed to validate the reliability of the proposed approach. Finally, the effectiveness of the approach is evaluated by comparing the results of the proposed model in this paper, the fuzzy comprehensive evaluation (FCE), the Bayesian Networks (BNs), and evidence theory.

4.1 Case Analysis

We invited six information system experts, two of which are also IT managers of the company, to assess the security risk of the company's information systems. As mentioned in Section 3.1, the ISS index system and weights have been established based on the risk analysis for this securities company (see Table 1).

Furthermore, based upon the ISS index system, an evidential diagram (see Figure 3) for the main assertion "ISS risk" was developed. In Figure 3, we used the "and" relationship between the main assertion and the subassertions, which implies that the main assertion is true if and only if all subassertions are true.

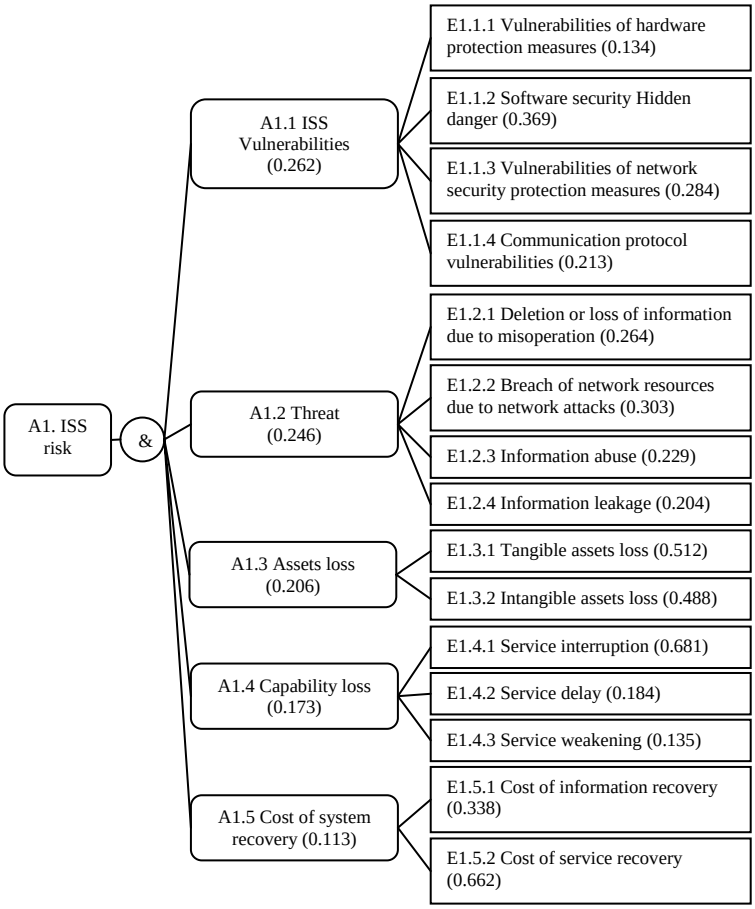

Figure 3. Evidential diagram for the main assertion "ISS risk".

According to the evidential diagram, we defined the frame of discernment of the assertions as Θ = {very high risk, high risk, median risk, low risk, very low risk}, where A_1={very high risk}, A_2={high risk}, A_3={median risk}, A_4={low risk}, and A_5={very low risk}. With the exception of A_1 to A_5, other subsets of $P(\Theta)$, noted by U, represent the unknown degree of evidence.

Six experts assessed the strength of evidence, which indicate the level of support that an item of evidence provides. For simplicity, we illustrated the process of reasoning by the strength of an item of evidence provided by one expert.

Strength of evidence is represented by fuzzy form. In this case study, we employed asymmetric triangular membership function [28] to describe the belief degree of evidence. As shown in Figure 4, the membership values of the evidence E, E = {e_1, e_2,…, e_{15}}, are provided by an expert. $\tilde{F}_1$ to $\tilde{F}_5$ are defined as the fuzzy subsets on E and the level

of risk of $\tilde{F}_k$ is higher than $\tilde{F}_{k-1}$. Then, based on Proposition 1, the BBAs for subassertions A1.1 to A1.5 were computed (see Table 2).

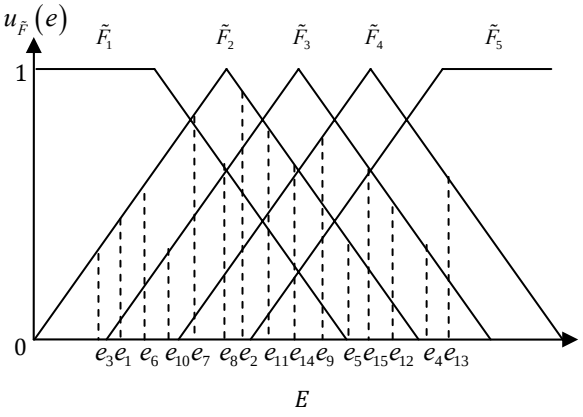

Figure 4. Membership function.

Table 2. The BBAs for the subassertions.

Sub-assertion	$m(A_1)$	$m(A_2)$	$m(A_3)$	$m(A_4)$	$m(A_5)$	$m(U)$
A1.1	0.107	0.216	0.203	0.215	0.172	0.077
A1.2	0.093	0.177	0.130	0.345	0.208	0.047
A1.3	0.069	0.131	0.169	0.251	0.257	0.123
A1.4	0.132	0.147	0.206	0.331	0.149	0.035
A1.5	0.070	0.131	0.133	0.298	0.332	0.036

The BBAs for main assertion "ISS risk" are computed by combining the BBAs of the subassertions based on the structure of Figure 3. This is done by propagating the BBAs through the network. Shenoy and Shafer [29] discussed this process in detail. The process of propagating BBAs in a network becomes computationally quite complex. However, there are several software packages available [30, 31] that facilitate the process. We use the tool for propagating uncertainty in valuation networks [30] to conduct the computation. The BBAs for main assertion "ISS risk" are $m(A_1) = 0.049$, $m(A_2) = 0.162$, $m(A_3) = 0.214$, $m(A_4) = 0.316$, $m(A_5) = 0.217$, and $m(U) = 0.042$.

Similarly, we could also obtain the BBAs according to the strength of evidence provided by other five experts (see Table 3).

Table 3. The BBAs for main assertion "ISS risk".

Experts	$m(A_1)$	$m(A_2)$	$m(A_3)$	$m(A_4)$	$m(A_5)$	$m(U)$
Expert1(m_1)	0.049	0.162	0.214	0.316	0.217	0.042
Expert2(m_2)	0.039	0.169	0.220	0.323	0.198	0.051
Expert3(m_3)	0.098	0.104	0.199	0.248	0.254	0.097
Expert4(m_4)	0.102	0.153	0.296	0.207	0.186	0.056
Expert5(m_5)	0.065	0.112	0.186	0.298	0.203	0.136
Expert6(m_6)	0.053	0.142	0.221	0.300	0.204	0.080

Then, we tested the consistency of above six items of evidence from m_1 to m_6 as mentioned in Section 3.4. Since there were only six experts participating in the risk assessment, we set a higher threshold ξ, $\xi = 0.85$. According to Table 3 and Eqs. (9) to (12), we obtained the similarity matrix:

$$SM = \begin{bmatrix} 1 & 0.816 & 0.801 & 0.754 & 0.832 & 0.817 \\ 0.816 & 1 & 0.853 & 0.844 & 0.781 & 0.776 \\ 0.801 & 0.853 & 1 & 0.696 & 0.798 & 0.800 \\ 0.754 & 0.844 & 0.696 & 1 & 0.821 & 0.755 \\ 0.832 & 0.781 & 0.798 & 0.821 & 1 & 0.829 \\ 0.817 & 0.776 & 0.800 & 0.755 & 0.829 & 1 \end{bmatrix}.$$

It is obvious that the similarity of any two items of evidence is lesser than ξ. Therefore, we have to adjust the existing items of evidence. The results of adjustment are as follows:

(1) Based on Eqs. (13) and (14), the credibility of the items of evidence are:

$C(m_1) = 0.243$, $C(m_2) = 0.216$, $C(m_3) = 0.109$, $C(m_4) = 0.045$, $C(m_5) = 0.186$, and $C(m_6) = 0.201$.

(2) Weighted average for BBAs of the items of evidence:

$m_{MAE}(A_1) = 0.058$, $m_{MAE}(A_2) = 0.143$, $m_{MAE}(A_3) = 0.214$, $m_{MAE}(A_4) = 0.311$, $m_{MAE}(A_5) = 0.210$, and $m_{MAE}(U) = 0.064$.

(3) Combine the weighted average evidence five times:

$m(A_1) = 0.032$, $m(A_2) = 0.138$, $m(A_3) = 0.223$, $m(A_4) = 0.416$, $m(A_5) = 0.165$, and $m(U) = 0.026$.

Consequently, the results of ISS risk assessment in this case study is shown in Figure 5, in which the belief supporting A_4, i.e. "ISS risk is low", is 0.416. This suggests that we have the most confidence that the ISS risk is low.

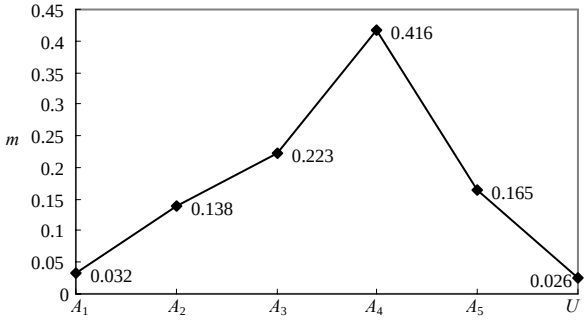

Figure 5. Results of the ISS risk assessment.

4.2 Sensitivity Analysis

In this section, we perform sensitivity analysis to investigate how the change of the strength of evidence affects the result of the ISS risk assessment.

For instance, we decreased the strengths of E1.4.3 and E1.4.1 (see in Figure 3), and then examined the impact of the change of the strength on the beliefs of the main assertion "A1. ISS risk" respectively.

The corresponding results are shown in Figure 6 and Figure 7.

The results in Figure 6 and Figure 7 indicate that although the strengths of E1.4.3 and E1.4.1 have been changed, the belief supporting A4 is still lager than others. Furthermore, by comparing Figure 6 with Figure 7, we can also observe that the larger the weight of evidence, the larger the impact on the belief of the main assertion is, as shown in Figure 3 where the weights of E1.4.3 and E1.4.1 are 0.135 and 0.681 respectively.

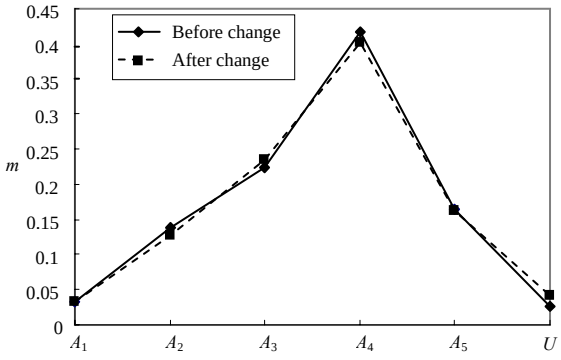

Figure 6. Impact of the change of E1.4.3 strength on the main assertion.

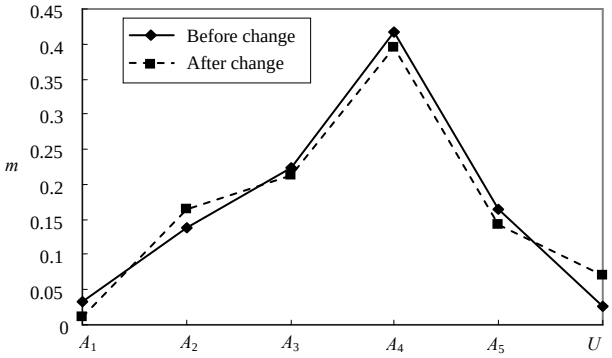

Figure 7. Impact of the change of E1.4.1 strength on the main assertion.

In addition, we have also performed sensitivity analysis to investigate how the strengths of other items of evidence affected the beliefs on the main assertions. The results showed that the small variations in the input strengths of evidence do not impact significantly the beliefs of the main assertion. This implies that the approach is robust and reliable to small amounts of measurement error in assessing strength of evidence.

4.3 Evaluation of the Hybrid Approach

Under the same conditions, we have employed the FCE, the BNs, and evidence theory to assess the ISS risk in this case study.

In particular, we use Method1, Method2, Method3, and Method4 to refer to our proposed approach, FCE, BNs, and evidence theory respectively.

Firstly, we compared the Method1 with the Method2 and the Method3 (see Figure 8).

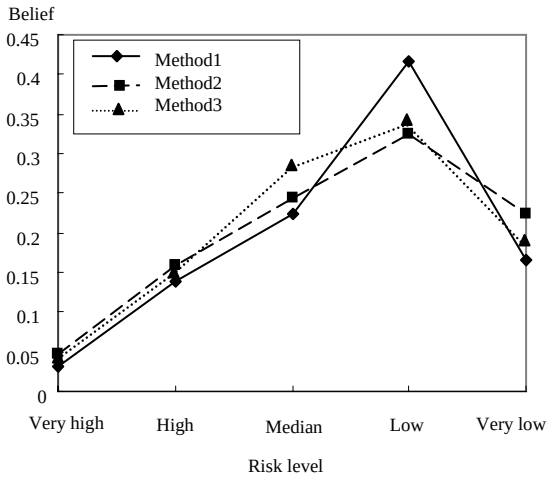

Figure 8. Comparison of the Methodl, the Method2, and the Method3.

The assessment results indicated that the sequences of risk level obtained from three methods are consistent. Furthermore, we can also observe that the degree of the belief of low rīsk level is higher in the Method1 than in the Method2 and the Method3, while the degrees of the belief of other levels are lower in the Method1 than in the Method2 and the Method3. Therefore, the Method1 is more effective than the other two methods in the ISS risk assessment in e-business.

Secondly, we compared the Method1 with the Method4 (see Figure 9).

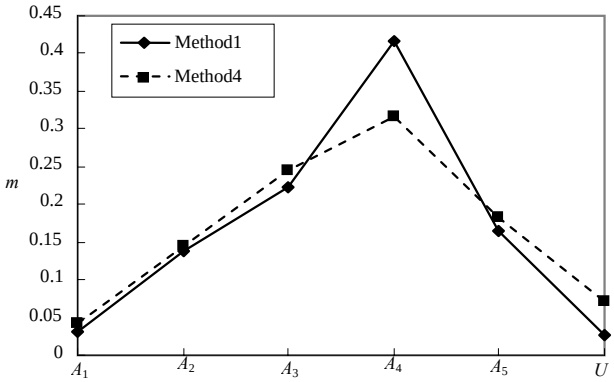

Figure 9. Comparison of the Method1 and the Method4.

The experiment results show that our proposed approach combining evidence theory with fuzzy sets outperforms evidence theory method in the ISS risk assessment in e-business. Moreover, in Figure 9, we can also find that the *m* value of *U* in the Method1 is higher than that in the Method4. Thus, in the ISS risk assessment, there is lower uncertainty in the Method1 than in the Method4.

5. Conclusions

In this paper, we propose a hybrid approach that combines the evidence theory with fuzzy sets for ISS risk assessment in electronic business. This approach has several advantages. First, the approach is based on evidence theory and fuzzy sets, which can effectively model the uncertainty involved in the assessment process in e-business. Second, for dealing with fuzzy evidence found in the ISS risk assessment, this approach provides a new way to define the basic belief assignment in fuzzy measure. Further, this approach also provides a method of testing the evidential consistency, which can reduce the uncertainty derived from the conflicts of evidence provided by experts.

In this paper, we also employed the sensitivity analysis to validate the reliability of the proposed approach. In addition, the effectiveness of the approach is evaluated by comparing the results of risk assessment of the proposed approach in this paper, FCE, BNs, and evidence theory.

Although the proposed approach performs with an advantage over existing methods in e-business environment, it still requires domain experts' belief inputs at the individual evidence level. Future research will be conducted to explore how to better elicit practitioners' assessments of the strength of the evidence.

Acknowledgements

The research was supported by the National Natural Science Foundation of China (Grant No. 70901054). The authors are very grateful to all anonymous reviewers whose invaluable comments and suggestions substantially helped improve the quality of the paper.

References

[1] A. Kankanhalli, H. H. Teo, B. C.Y. Tan, K. K. Wei, An integrative study of information systems security effectiveness, International Journal of Information Management 23(2) (2003) 139-154.

[2] M. Karyda, E. Kiountouzis, S. Kokolakis, Information systems security policies: A contextual perspective, Computers and Security 24(3) (2005) 246-260.

[3] D.W. Straub, R.J. Welke, Coping with systems risk: Security planning models for management decision-making, MIS Quarterly 22(4) (1998) 441-469.

[4] R. L. Winkler, Uncertainty in probabilistic risk assessment, Reliability Engineering and System Safety 54(2-3) (1996) 127-132.

[5] R. K. Rainer, C. A. Snyder, H. H. Carr, Risk analysis for information technology, Journal of Management Information Systems 8(1) (1991) 129–147.

[6] L. D. Bodin, L. A. Gordon, M. P. Loeb, Information security and risk management, Communications of the ACM 51(4) (2008) 64-68.

[7] G. V. Post, J. D. Diltz, A stochastic dominance approach to risk analysis of computer systems, MIS Quarterly 10(4) (2001) 363–375.

[8] Y. Huanchun, Risk evaluation model on enterprises' complex information system: a study based on the BP neural network, Journal of Software 5(1) (2010) 99-106.

[9] L. Grunske, D. Joyce, Quantitative risk-based security prediction for component-based systems with explicitly modeled attack profiles, Journal of Systems and Software 81(8) (2008) 1327-1345.

[10] W. G. de Ru, J. H. P. Eloff, Risk analysis modeling with the use of fuzzy logic, Computers and Security 15(3) (1996) 239-248.

[11] D. Xu, J. Sha, P. Zhang, B. Wan, Study of switch project construction risk identification evaluation and tacking based on Delphi method, System Engineering Theory and Practice 20(12) (2000) 113-118.

[12] D. K. Hardman, P. Ayton, Arguments for qualitative risk assessment: the StAR risk adviser, Expert Systems 14(1) (2000) 24-36.

[13] S. Alter, S. Sherer, A general, but readily adaptable model of information system risk, Communications of the AIS 14(1) (2004) 1–28.

[14] H. Salmela, Analysing business losses caused by information systems risk: a business process analysis approach, Journal of Information Technology 23(3) (2008) 185-202.

[15] C. Fan, Y. Yu, BBN-based software project risk management, Journal of Systems and Software 73(2) (2004) 193-203.

[16] Y. Hu, J. Chen, H. Jiaxing, L. Mei, X. Kang, Analyzing software system quality risk using Bayesian belief network, in: Proceedings of the 2007 IEEE International Conference on Granular Computing, 2007, pp. 93-96.

[17] E. Lee, Y. Park, J. Shin, Large engineering project risk management using a Bayesian belief network, Expert Systems with Applications 36(3) (2009) 5880-5887.

[18] T. Zhan, X. Wang, Risk assessment for traffic information security based on fuzzy comprehensive evaluation, in: Proceedings of the 2nd International Conference on Transportation Engineering, 2009, pp. 3809-3814.

[19] T. R. Peltier, Information Security Risk Analysis, second ed., CRC press, Boca Raton, 2007.

[20] X. Yang, H. Luo, C. Fan, M. Chen, S. Zhou, Analysis of risk evaluation techniques on information system security, Journal of Computer Applications 28(8) (2008) 1920-1924.

[21] G. Shafer, The Dempster-Shafer theory, in: S.C. Shapiro (ed.), Encyclopedia of Artificial Intelligence, John Wiley and Sons, New York, 1992, pp. 330–331.

[22] A. L. Jousselme, D. Grenier, E. Bosse, A new

distance between two bodies of evidence, Information fusion 2(1) (2001) 91-101.
[23] R. L. Kumar, S. Park, C. Subramaniam, Understanding the value of countermeasure portfolios in information systems security, Journal of Management Information Systems 25(2) (2008) 241-279.
[24] Z. S. Xu, A method for priorities of triangular fuzzy number complementary judgment matrices, Fuzzy Systems and Mathematics 16(1) (2002) 55-60.
[25] L. Zhou, A. Vasconcelos, M. Nunes, Supporting decision making in risk management through an evidence-based information systems project risk checklist, Information Management and Computer Security 16(2) (2008) 166-186.
[26] J. W. Guan, D. A. Bell, Approximate reasoning and evidence theory, Information sciences 96(3-4) (1997) 207-235.
[27] C. K. Murphy, Combining belief functions when evidence conflicts, Decision support systems, 29(1) (2000) 1-9.
[28] C. G. Jin, Y. Lin, Z. S. Ji, Application of event tree analysis based on fuzzy sets in risk analysis, Journal of Dalian University of Technology 43(1) (2003) 97-100.
[29] P. P. Shenoy, G. Shafer, Axioms for probability and belief-function propagation, Uncertainty in Artificial Intelligence 4 (1990) 169-198.
[30] A. Saffiotti, E. P. Umkehrer, A general tool for propagating uncertainty in valuation networks, in: Proceedings of the Seventh National Conference on Artificial Intelligence, 1991, pp. 323-331.
[31] G. Shafer, P. P. Shenoy, R. P. Srivastava, Auditor's Assistant: A knowledge engineering tool for audit decisions, in: Proceedings of the 1988 Touche Ross/University of Kansas Symposium on Auditing Problems, 1988, pp. 61-79.